

Recopilación Pasiva de Información utilizando Google Hacking y Shodan



Índice

Enunciado de la tarea.....	3
Resolución de la tarea.....	4
Ejercicio 1.....	4
Ejercicio 2.....	7
Ejercicio 3.....	9
Reflexión ética.....	12

Enunciado de la tarea

Tarea: Recopilación Pasiva de Información utilizando Google Hacking y Shodan

Objetivos:

Aplicar los conocimientos teóricos sobre la recopilación pasiva de información en un ejercicio práctico.

Explorar y utilizar técnicas de Google Hacking para la obtención de información sensible y expuesta en Internet.

Aprender a usar Shodan para identificar dispositivos y servicios expuestos públicamente.

Reflexionar sobre las implicaciones éticas del uso de estas herramientas.

Instrucciones:

Parte 1: Google Hacking

Búsqueda en Google:

Elige una organización ficticia o real (para la cual tienes autorización). Utiliza los comandos avanzados de Google para recopilar información pasiva.

Realiza al menos 5 búsquedas avanzadas utilizando comandos como site:, filetype:, intext: y combinaciones de operadores booleanos como OR o -.

Documenta tus búsquedas y los resultados obtenidos en un informe. Nota: No utilices estas técnicas en sitios no autorizados(contenido para adultos, web del Centro, o páginas de contenido ilícito).

Consulta con Google Dorks:

Accede a la Google Hacking Database (GHDB) en el sitio de Exploit DB. Selecciona 3 Google Dorks que te parezcan relevantes para obtener información sensible, como contraseñas, archivos de configuración, o datos expuestos en servicios como Trello o GitHub.

Realiza las búsquedas en Google y documenta los resultados, siempre garantizando la legalidad y la ética de las búsquedas.

Parte 2: Shodan

Exploración de Shodan:

Crea una cuenta gratuita en Shodan.io (si no la tienes ya).

Realiza 3 búsquedas avanzadas en Shodan, usando filtros como port:, country:, o org:, para identificar dispositivos o servicios expuestos en internet.

Por ejemplo, puedes buscar servidores FTP o cámaras IP expuestas.

Documenta las IPs encontradas, su ubicación geográfica y cualquier información adicional relevante. No intentes interactuar con los dispositivos que encuentres.

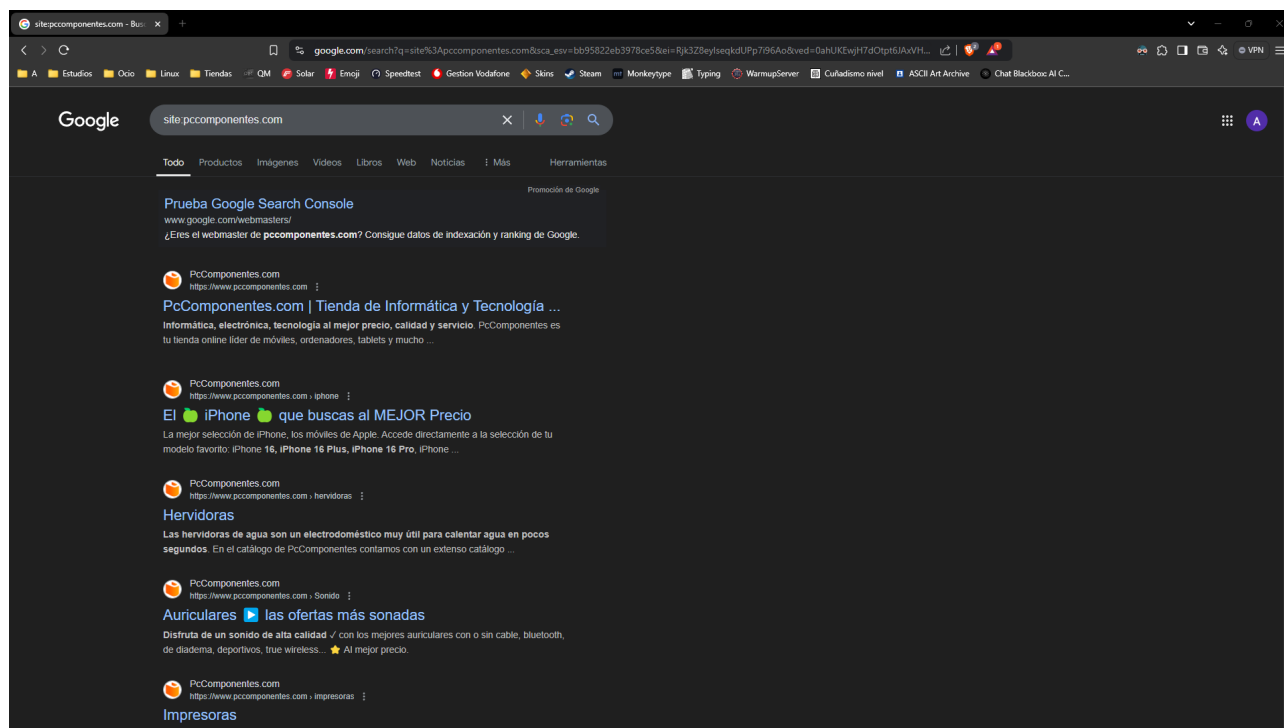
Parte 3: Reflexión ética

Redacta un breve ensayo (máximo 500 palabras) reflexionando sobre los posibles riesgos y consecuencias de utilizar herramientas como Google Hacking y Shodan en sistemas no autorizados. ¿Cuáles son las responsabilidades éticas y legales de un hacker ético en este contexto?

Resolución de la tarea

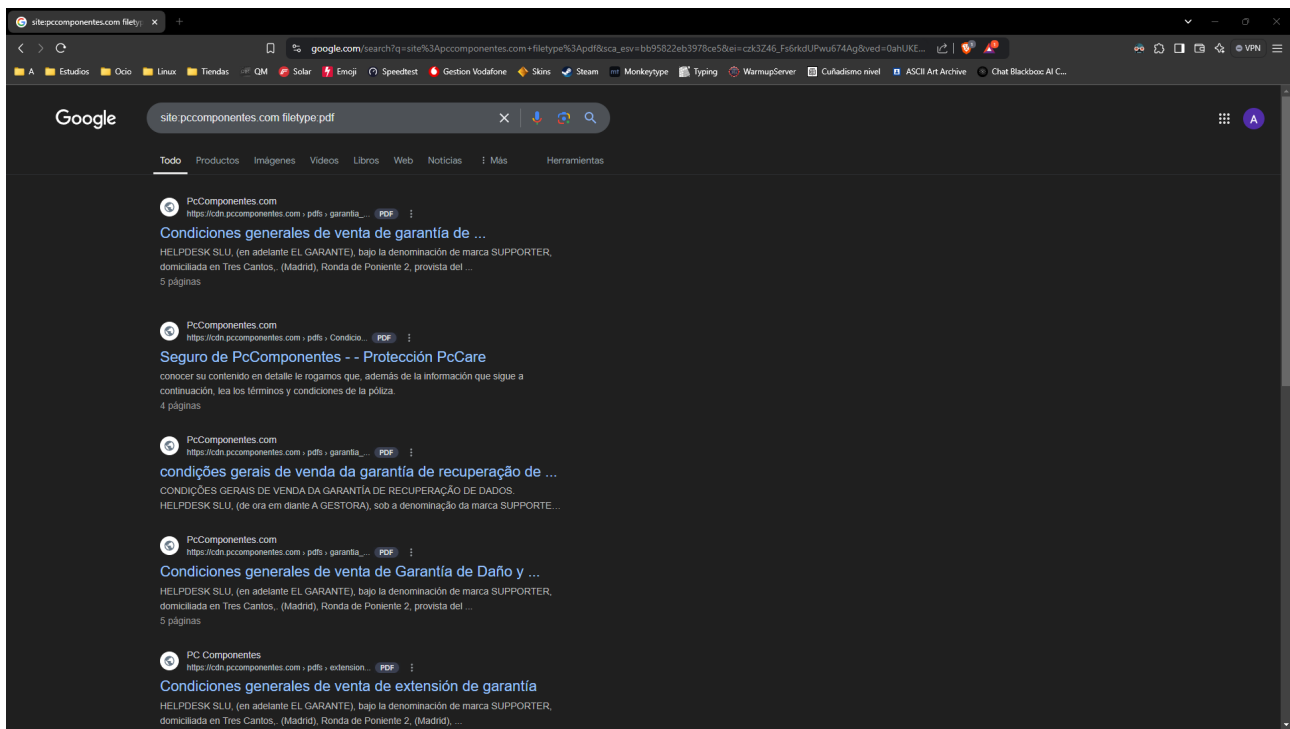
Ejercicio 1

Voy a usar una organización llamada PcComponentes, para ello primero voy a buscar la página PcComponentes, por medio del comando site.

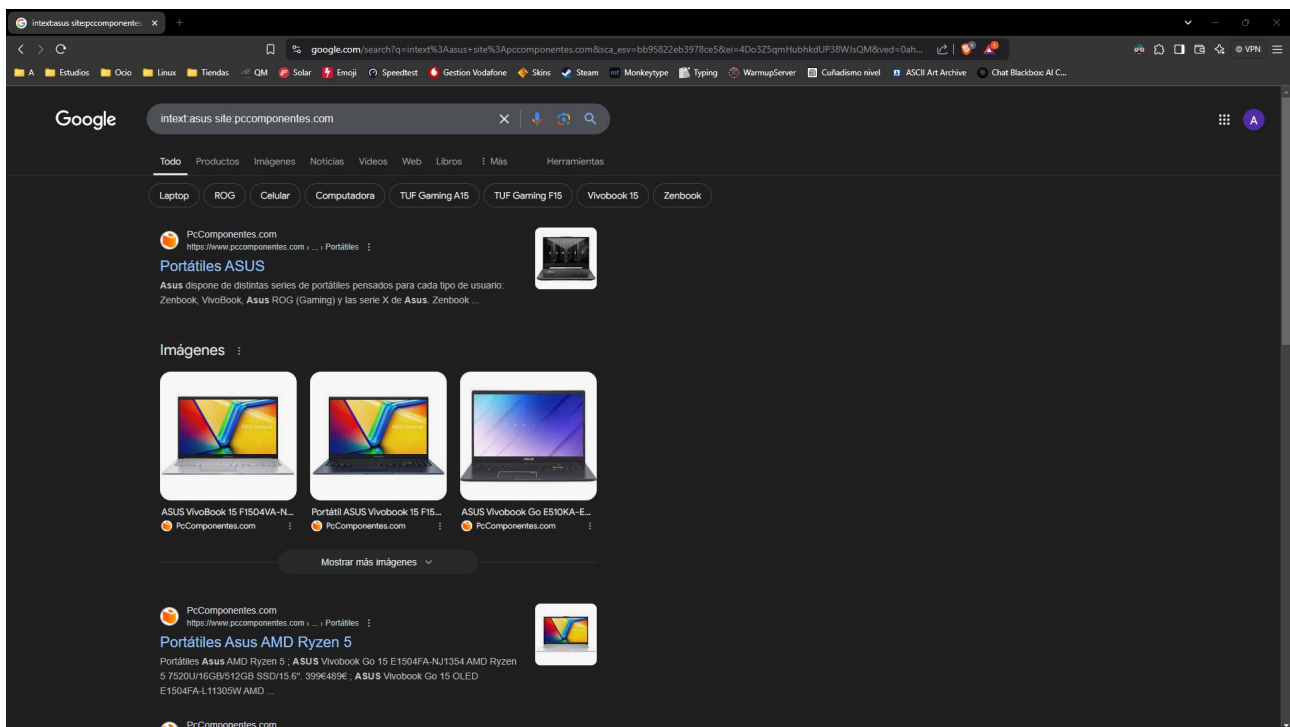


Al buscar de esta forma, únicamente me muestra resultado acerca de la página pccomponentes.com.

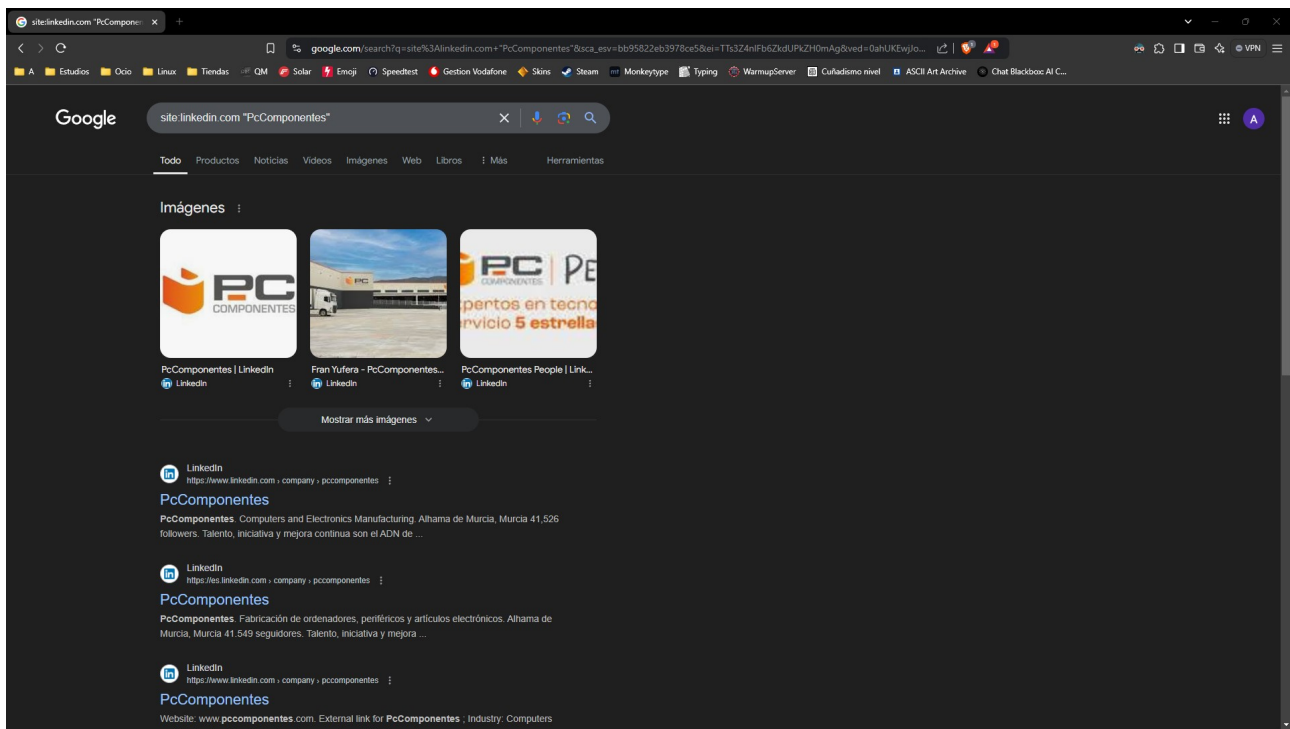
Ahora a continuación voy a mostrar los archivos pdf por ejemplo que tengan en PcComponentes.



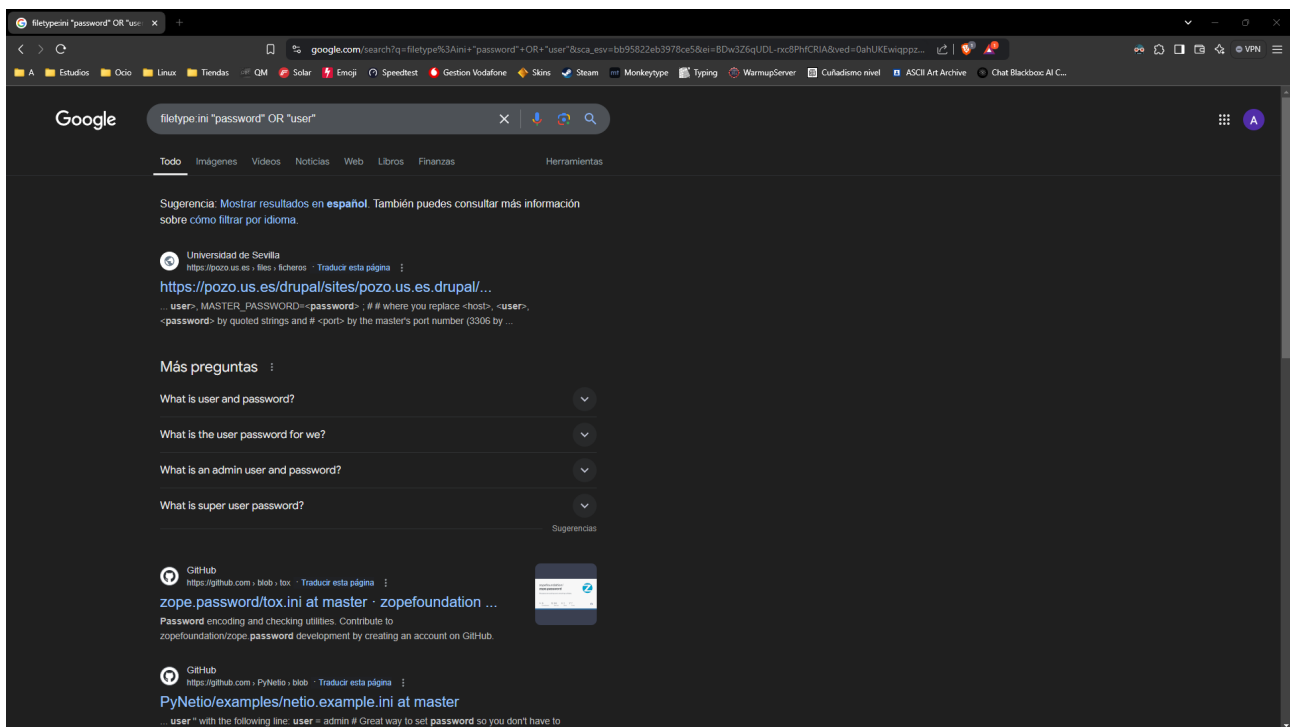
Ahora he usado el comando filetype, y he especificado la extensión pdf, de tal manera que me va a mostrar únicamente los archivos pdf que tenga públicos la página PcComponentes.



Con esta búsqueda, al poner el comando intext le estoy diciendo, que dentro del dominio especificado, me muestre todas las páginas que contengan algo relacionado con Asus.



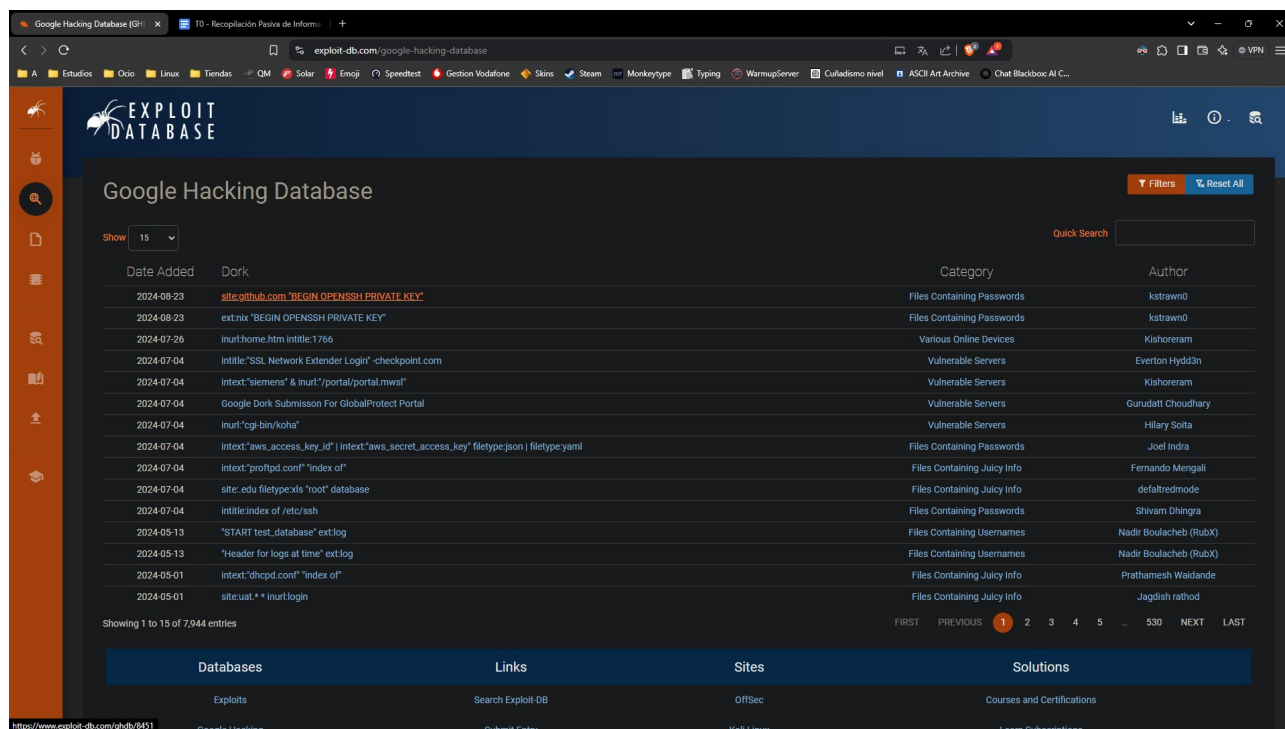
Al ponerle site:linkedin.com “PcComponentes”, me muestra perfiles de linkedin relacionados con PcComponentes, ya sea la cuenta de la misma empresa, o cuentas de trabajadores que trabajen en PcComponentes.



Ahora no he podido buscar a través de la página PcComponentes, ya que no muestra públicos archivos ini, por eso le he quitado el comando de site, pero al poner únicamente filetype:ini “password” OR “user”, estoy diciendo que me muestre los archivos ini que contentan esos parámetros.

Muchos de estos comandos se pueden combinar para obtener más información acerca de una página.

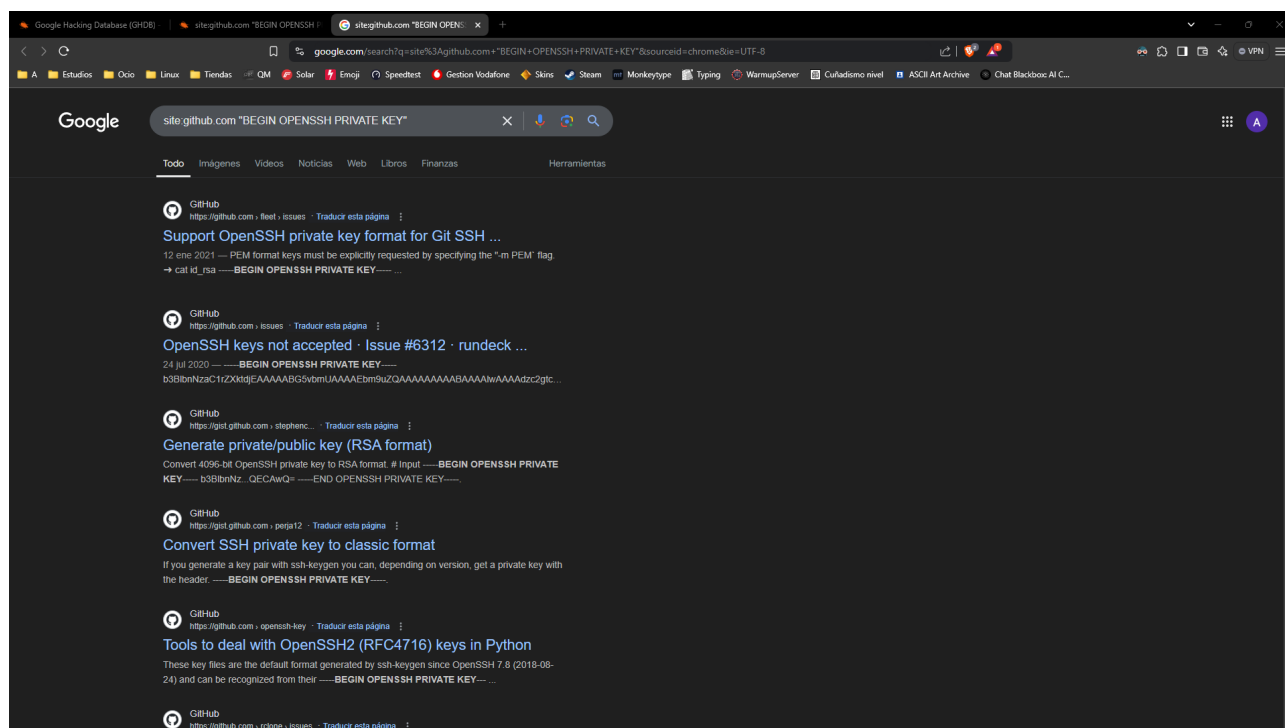
Ejercicio 2



The screenshot shows the Exploit Database website interface. The search bar at the top contains the text "Google Hacking Database". Below the search bar, there is a table of search results. The table has columns for "Date Added", "Dork", "Category", and "Author". The first row shows a dork "site:github.com 'BEGIN OPENSSSH PRIVATE KEY'" added on 2024-08-23, categorized as "Files Containing Passwords", and authored by "kstrawn0".

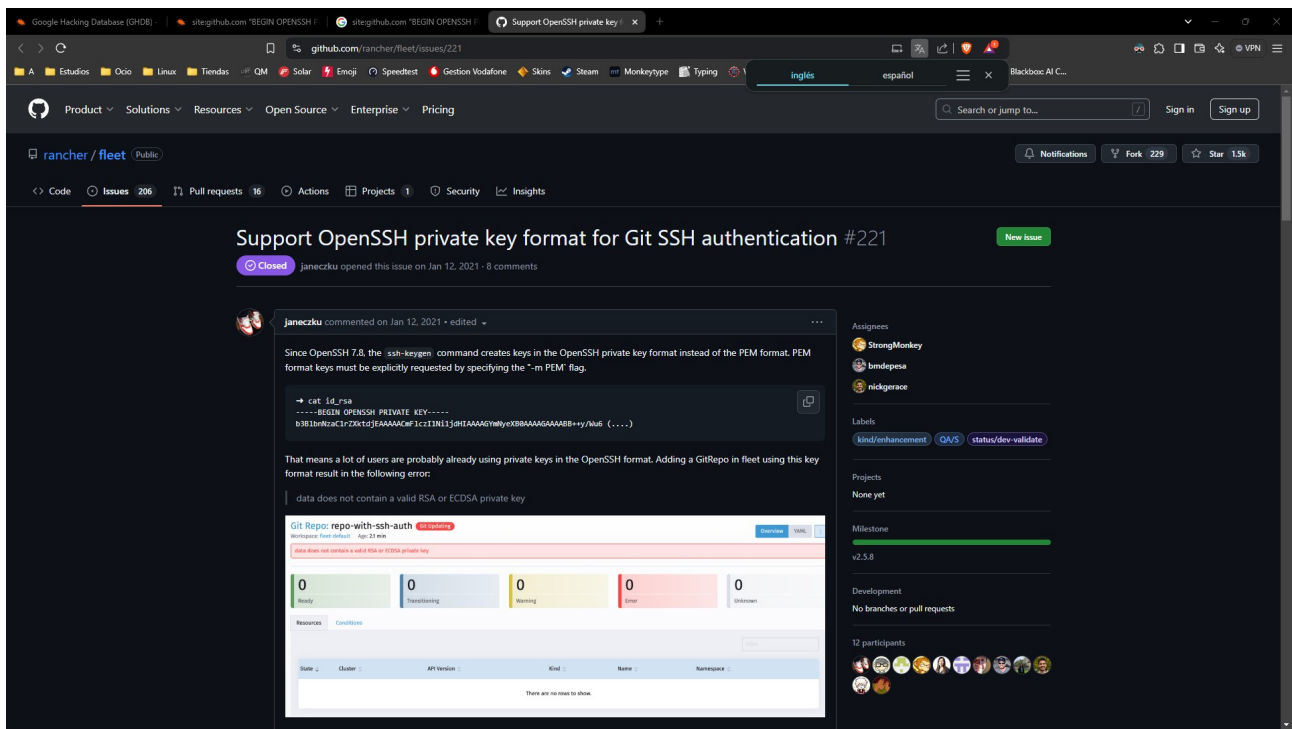
Date Added	Dork	Category	Author
2024-08-23	site:github.com "BEGIN OPENSSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-08-23	ext:nix "BEGIN OPENSSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices	Kishoreram
2024-07-04	intitle:"SSL Network Extender Login" -checkpoint.com	Vulnerable Servers	Everton Hydd3n
2024-07-04	intext:"siemens" & inurl:"portal/portal.mwsl"	Vulnerable Servers	Kishoreram
2024-07-04	Google Dork Submission For GlobalProtect Portal	Vulnerable Servers	Gurudatt Choudhary
2024-07-04	inurl:"cgi-bin/koha"	Vulnerable Servers	Hilary Soita
2024-07-04	intext:"aws_access_key_id" intext:"aws_secret_access_key" filetype:json filetype:yaml	Files Containing Passwords	Joel Indra
2024-07-04	intext:"proftpd.conf" "index of"	Files Containing Juicy Info	Fernando Mengali
2024-07-04	site:.edu filetype:xls "root" database	Files Containing Juicy Info	defaultmode
2024-07-04	intitle:index of /etc/ssh	Files Containing Passwords	Shivam Dhingra
2024-05-13	"START test_database" ext:log	Files Containing Usernames	Nadir Boulacheb (RubX)
2024-05-13	"Header for logs at time" ext:log	Files Containing Usernames	Nadir Boulacheb (RubX)
2024-05-01	intext:"dhcpd.conf" "index of"	Files Containing Juicy Info	Prathamesh Waidande
2024-05-01	site:uat.* * inurl:login	Files Containing Juicy Info	Jagdish rathod

En la página Exploit DB, busco Google Hacking, y accedo a la base de datos de Google Hacking.

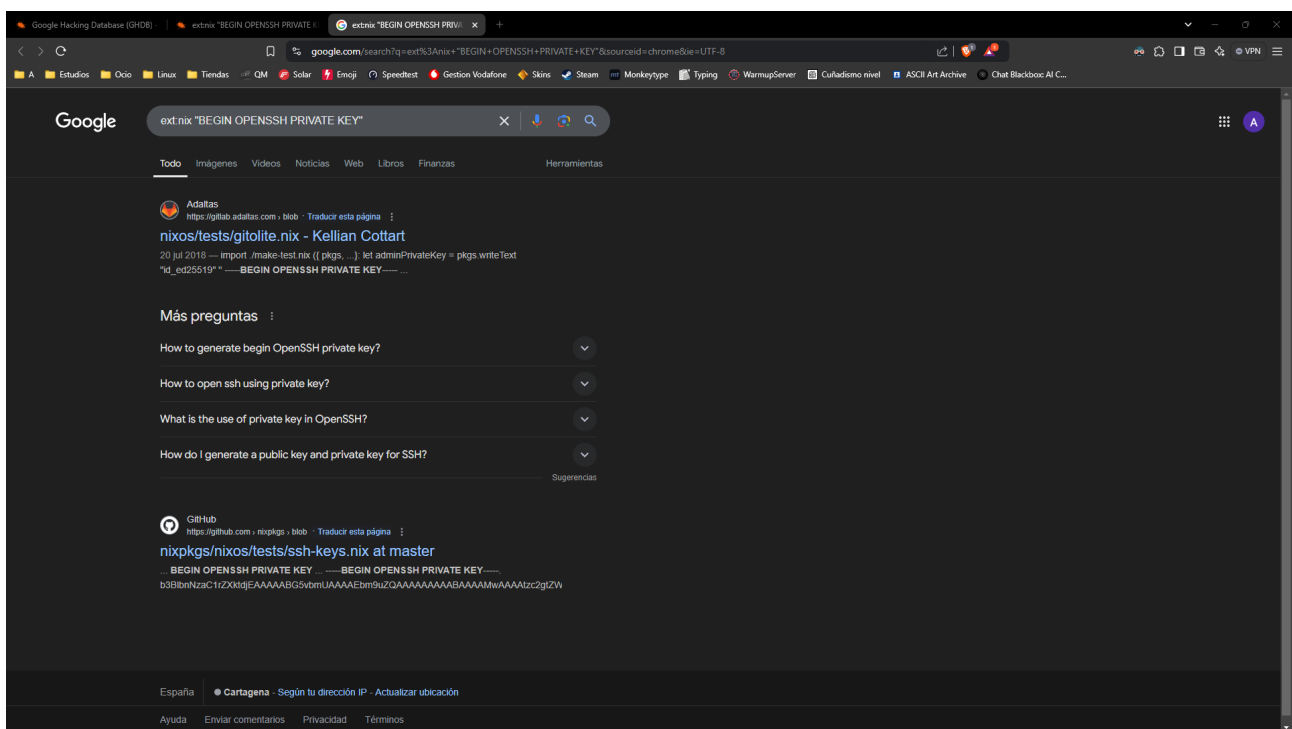


The screenshot shows a Google search results page for the query "site:github.com 'BEGIN OPENSSSH PRIVATE KEY'". The search results are displayed in a list format. The first result is from GitHub, titled "Support OpenSSH private key format for Git SSH ...". The second result is from GitHub, titled "OpenSSH keys not accepted · Issue #6312 · Rundeck ...". The third result is from GitHub, titled "Generate private/public key (RSA format)". The fourth result is from GitHub, titled "Convert SSH private key to classic format". The fifth result is from GitHub, titled "Tools to deal with OpenSSH2 (RFC4716) keys in Python".

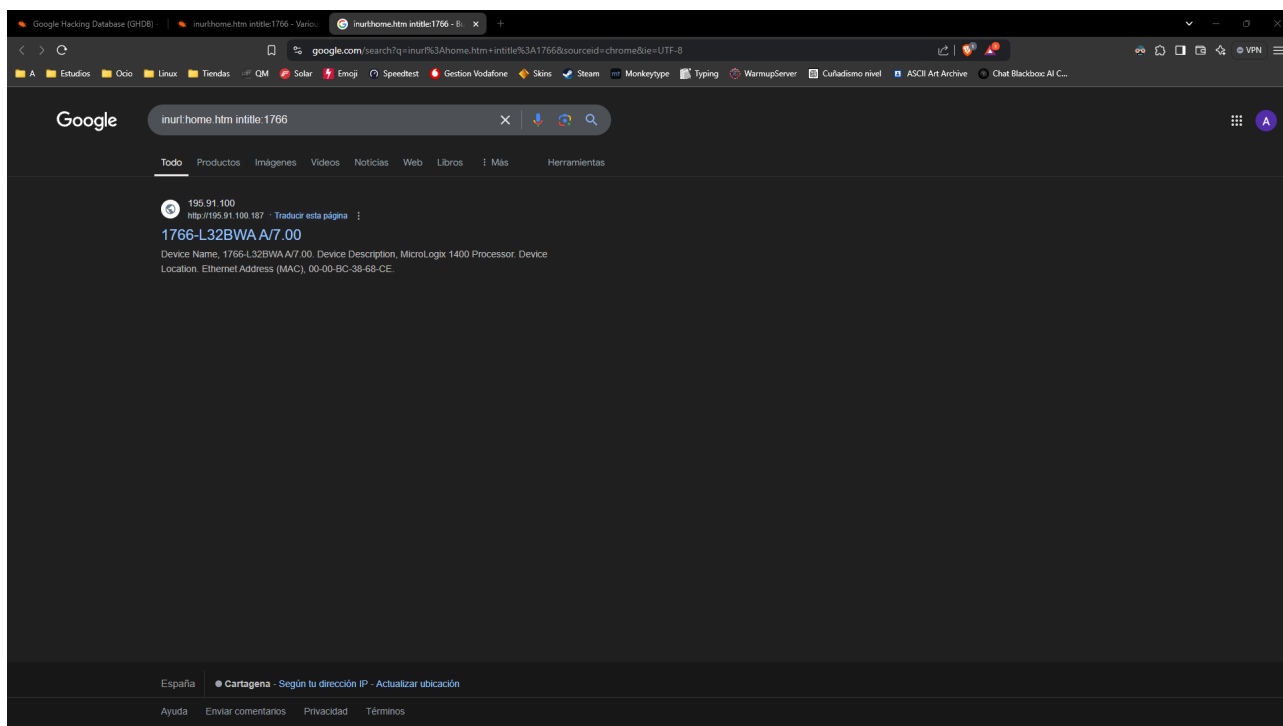
He elegida por ejemplo la primera línea de la base de datos, que es de un repositorio de GitHub.



Aquí en este repositorio de GitHub, podemos ver un rsa privado de ssh.

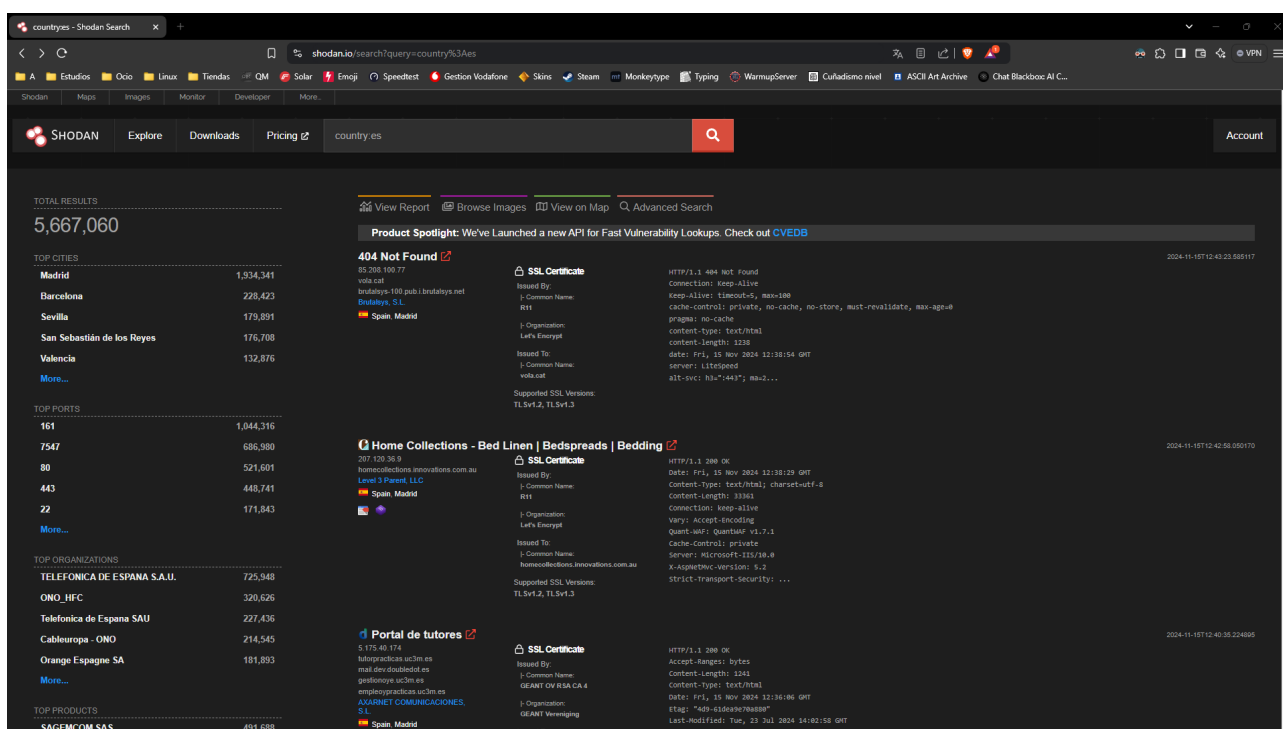


Este es otro Google Dork, también mostrado en la página ExploitDB

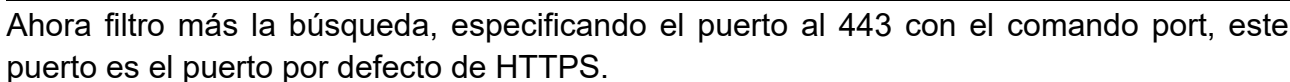
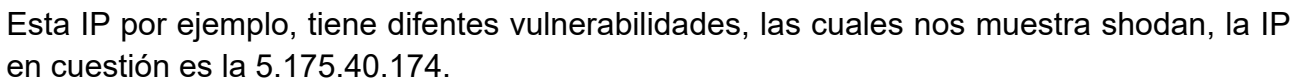


Y este de aquí es otro, Google Dork.

Ejercicio 3



A continuación voy a utilizar el programa shodan, el cuál es muy potente para detectar vulnerabilidades de diferentes IPs o páginas web. En este caso he buscado con el comando country todas las IPs que tengan un puerto abierto, ya sea el 8080 (por defecto de internet) o cualquier otro.



Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2024

- CVE-2024-46898** falseSSRF in Apache HTTP Server on Windows with mod_rewrite in server/host context, allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue.
- CVE-2024-38477** falseNull pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- CVE-2024-38476** falseVulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerable to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- CVE-2024-38474** falseSubstitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.
- CVE-2024-27316** falseHTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

2023

- CVE-2023-45882** falseWhen a HTTP/2 stream was reset (RST frame) by a client, there was a time window where the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources

Apache httpd 2.4.52

Portal Templus

HTTP/1.1 200 OK
 Date: Fri, 15 Nov 2024 12:46:14 GMT
 Server: Apache/2.4.52 (Ubuntu)
 Cache-control: no-cache, private
 Vary: Accept-Language,Accept-Encoding
 Transfer-Encoding: chunked
 Content-Type: text/html; charset=utf-8

SSL Certificate

Certificate:
 Data:
 Version: 3 (x2)
 Serial Number:
 19:cb:d7:66:04:10:05:cc:16:10:44:32
 Signature Algorithm: sha256WithRSAEncryption
 Issuer: C=ES, O=GlobalSign nv-sa, CN=GlobalSign GCC R6 AlphaSSL CA 2023
 Validity
 Not Before: Feb 28 13:04:31 2024 GMT
 Not After : Mar 31 13:04:30 2025 GMT
 Subject: CN=*.templus.com
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (4096 bit)
 Modulus:
 00:0c:9f:66:3a:a8:1b:90:04:02:63:dc:cd:db:8a:
 a1:eb:0f:98:f2:4f:69:52:b3:16:4c:b3:1a:56:96:
 07:fb:08:28:48:4c:07:4c:79:c9:07:0f:0f:0c:1f:
 96:09:0c:05:fe:0b:79:16:22:19:61:88:32:0c:18:09:
 62:ad:f0:0d:77:76:5b:0b:f1:fe:08:30:04:2c:f3:
 5e:05:27:d1:0f:11:09:43:7c:68:fe:0c:f4:4c:95:
 0d:73:32:1c:66:33:07:32:0a:2a:52:12:0b:ea:0b:
 25:02:2b:0b:09:1a:0c:c5:0a:0f:00:02:0a:2b:3a:02:
 29:0d:01:0b:0e:8d:0f:93:04:39:03:0a:13:48:03:
 e5:0f:05:76:17:4e:43:27:3d:04:12:1c:f0:a8:eb:
 08:0d:10:3e:09:0f:4c:0c:ee:0f:24:5c:70:66:16:
 04:23:4f:0b:02:10:fa:04:10:3d:cd:0b:ea:cc:00:
 f2:29:0e:4c:cd:84:c8:54:34:42:05:0a:08:07:7a:
 04:95:02:07:23:ad:78:fa:59:59:03:0a:4d:23:af:
 73:34:2a:19:0d:70:13:04:0e:08:04:70:01:fe:70:
 2a:03:70:31:16:af:54:74:0e:27:28:13:2a:6c:0c:
 9a:b9:f8:cd:05:55:ea:a7:0b:06:5c:03:04:77:0f:
 19:05:0b:0f:30:0a:0a:1a:70:7a:03:0a:0a:13:03:

En este caso, esta IP tiene una cantidad grande de registros de vulnerabilidades, hay vulnerabilidades detectadas desde 2006.

SHODAN Explore Downloads Pricing country.es port.443 org Account

TOTAL RESULTS
908

TOP CITIES

Madrid	367
Barcelona	43
Zaragoza	28
Málaga	17
Alcobendas	16

TOP ORGANIZATIONS

Telefonica de Espana SAU	60
TELEFONICA DE ESPANA S.A.U.	47
arsys.es	40
Digi Spain Telecom	25
Amazon Data Services Spain	20

TOP PRODUCTS

Apache httpd	482
Apache Tomcat/Coyote JSP engine	36
nginx	34
lighttpd	26
Microsoft IIS httpd	23

TOP OPERATING SYSTEMS

Windows	31
---------	----

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

DADUN: Library - University of Navarra Home

51.92.127.221
 dadun.unav.edu
 e2-51-92-127-221.eu-south-2.com
 jule@unav.edu.es
 A169 BOW Inc
 Spain, Zaragoza

SSL Certificate

Issued By:
 J. Common Name: Seeligo ECC Organization
 Validation Secure Server CA
 J. Organization: Seeligo Limited
 Issued To:
 J. Common Name: dadun.unav.edu
 J. Organization: Universidad De Navarra
 Supported SSL Versions: TLSv1.2, TLSv1.3

HTTP/1.1 200 OK
 Date: Fri, 15 Nov 2024 12:28:08 GMT
 Server: Apache/2.4.52 (Ubuntu)
 X-Powered-By: Express
 X-Ratelimit-Limit: 500
 X-Ratelimit-Remaining: 499
 X-Ratelimit-Reset: 1731873715
 Link: <https://dadun.unav.edu/server/ldu/index>; rel="http://www.w3.org/ns/ldp#inbox"
 Content-Type: tex...

150.241.8.241

Fundacion Tecnika Research and Innovation
 Spain, Basauri

HTTP/1.1 200 OK
 Date: Fri, 15 Nov 2024 12:29:15 GMT
 Server: Apache/2.4.52 (Ubuntu)
 Last-Modified: Tue, 01 Oct 2024 07:12:49 GMT
 Etag: "29af-623658dc7064"
 Accept-Ranges: bytes
 Content-Length: 14671
 Vary: Accept-Encoding
 Content-Type: text/html

88.5.35.224

224 red-05-5-35-dynamic-ima-ida-ml
 Telefonica de Espana SAU
 Spain, Logroño

HTTP/1.1 200 OK
 Content-Type: text/html; charset=utf-8
 Referer-Policy: no-referrer
 X-Content-Type-Options: nosniff
 Server:

Al ponerle org, estoy diciendo que sea de una organizacion, lo que significa que el dominio es .org.

The screenshot shows a Shodan search result for the IP address 51.92.127.221. The left panel displays a list of vulnerabilities, categorized by year (2024 and 2013). The right panel shows the SSL certificate details for the IP address.

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2024

- CVE-2024-48898** falseSSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue.
- CVE-2024-38477** falsenull pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- CVE-2024-38476** falseVulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerable to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- CVE-2024-38474** falseSubstitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.
- CVE-2024-27316** falseHTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

2013

- CVE-2013-4365** Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- CVE-2013-2765** The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a

SSL Certificate

certificate:
Date:
Version: 3 (802)
Serial Number:
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Let's Encrypt, CN=Let's Encrypt
Subject: CN=51.92.127.221
Public Key Algorithm: RSA
Public Key: (RSA 2048)
X.509v3 extensions:
X.509v3 Authority Key Identifier:
X.509v3 Subject Key Identifier:
X.509v3 Key Usage: critical
X.509v3 Basic Constraints: critical
X.509v3 Extended Key Usage:
X.509v3 Certificate Policies:
X.509v3 CRL Distribution Points:
Full Name:
Authority Information Access:
CA Issuers - URI:
X.509v3 Subject Alternative Name:
CT Precertificate SCTs:
Signed Certificate Timestamp:

Este es el primer resultado que me ha mostrado esta búsqueda, hay también vulnerabilidades registradas, tanto de 2024, como desde 2013 hasta 2007, sin contar 2010 ni 2008.

Reflexión ética

Al buscar usando este tipo de filtros o comandos con herramientas como Google Hacking o Shodan, podemos acceder a sitios web a los cuales no estemos autorizados a entrar, lo cuál puede generar represalias para el buscador, hay recomendaciones si vas a entrar a sitios de ese tipo, como usar máquinas virtuales con adaptador NAT, utilizar navegadores como Tor, ya que pueden llegar a ocultar tu IP, no obstante hay que ser consciente de que siempre pueden llegar a rastrearte. Pero no es lo que buscamos nosotros, ya que el ámbito del Hacking se basa en fines éticos, con autorización de las personas a las que se les van a realizar auditorías utilizando técnicas como Pentesting o similares, de lo contrario, ya sería algo ilegal y no son los principios del Hacking, ya que pasar a ser Cibercriminal o Ciberdelincuente, este tipo de actos, afectan mucho a los hackers, ya que manchan su nombre, debido a que la gente llama hacker a los crackers, ciberdelincuentes, etc. A día de hoy, un hacker es muy importante, ya que puede detectar vulnerabilidades que a simple vista, para una persona sin conocimientos, no piensa que pueda tener, también hay que saber que nunca somos completamente invulnerables, ya que siempre que estemos conectados a internet, podemos recibir algún tipo de ataque, ya sea por técnicas como Phishing, Ataques DDoS, Troyanos, etc. por ello y por mucho más, en un empresa es recomendable que sólo sea administrador una persona con los conocimientos suficientes, para tomar medidas de precaución correctas para evitar dentro de lo posible poder ser atacado por un cibercriminal.